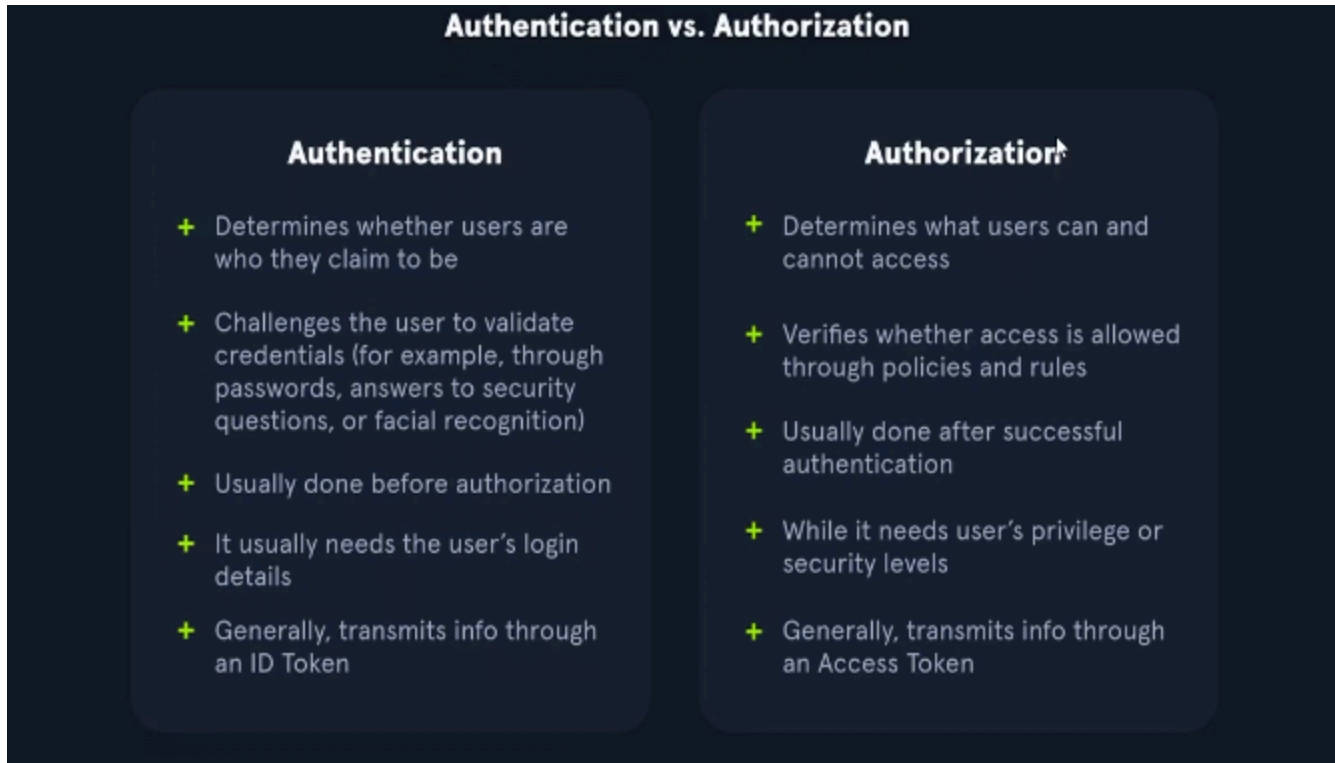


broken access control



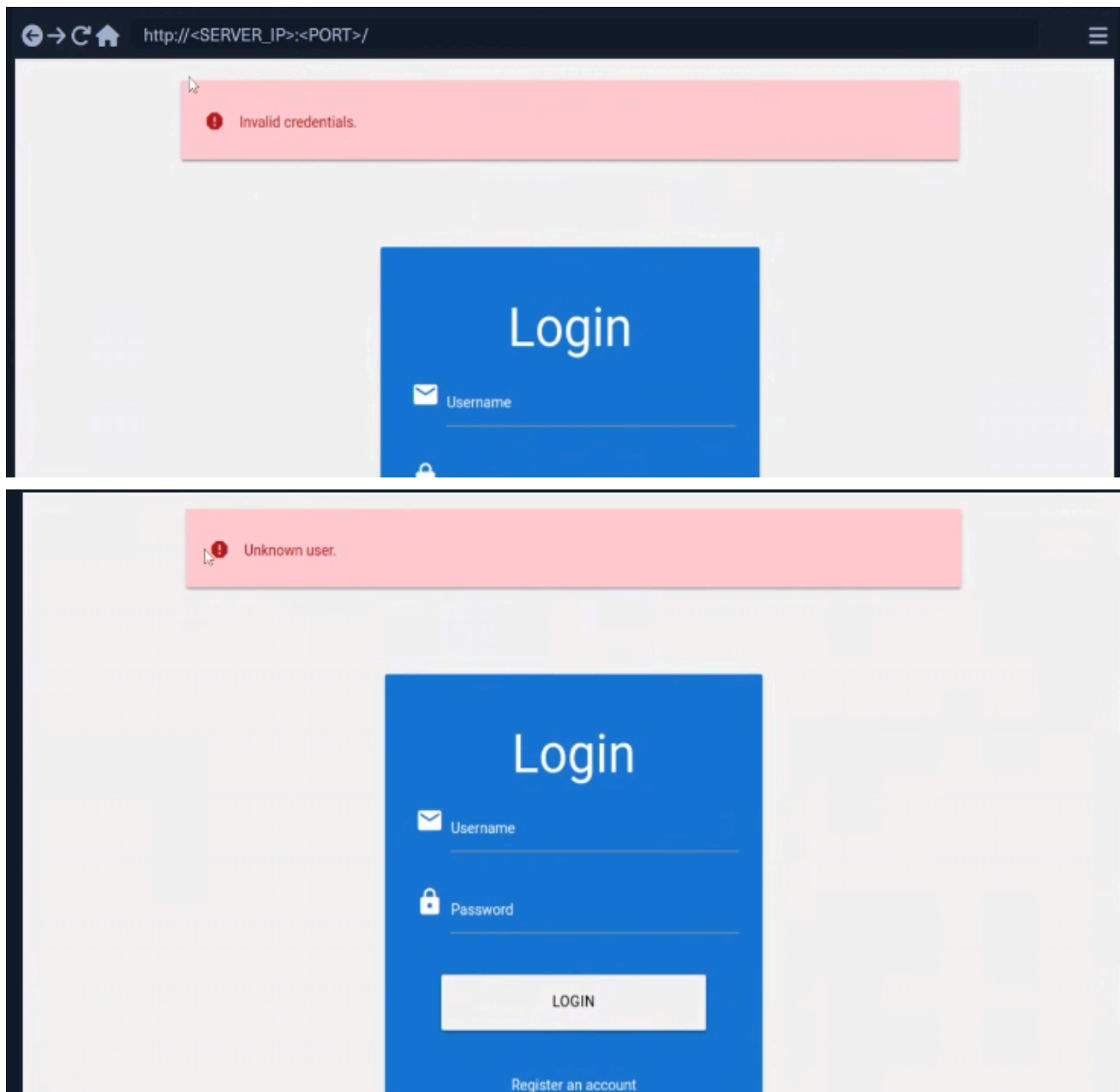
- هنا اول حاجه تعرف الفرق بين authentication authorization

• Authentication

- بتأكد إن المستخدم هو فعلاً الشخص المطلوب
- بتطلب من المستخدم يثبت هويته (زي الباسورد، سؤال أمان، بصمة، أو بصمة الوجه)
- دائماً بتحصل قبل التفويض (Authorization)
- بتحتاج بيانات دخول المستخدم (زي اليوزر نيم والباسورد)
- بتنقل البيانات غالباً باستخدام **ID Token**

Authorization

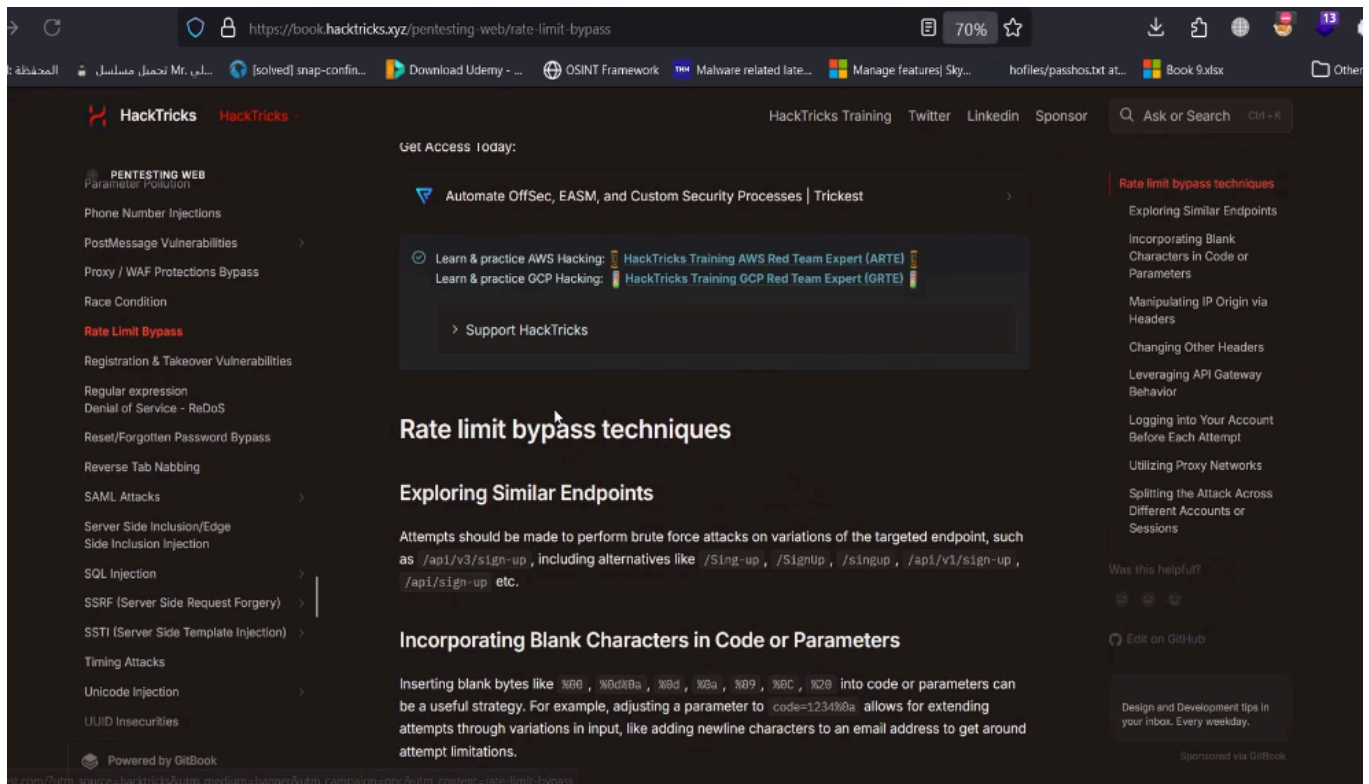
- بتحدد إيه اللي المستخدم يقدر يعمل أو يوصله
- بتراجع السياسات والقواعد علشان تشوف المستخدم له صلاحية ولا لأ.
- بتحصل بعد ما المستخدم يتأكد هويته (يعني بعد الـ Authentication).
- بتعتمد على صلاحيات المستخدم أو مستوى الأمان الخاص بيه.
- بتنقل البيانات غالباً باستخدام **Access Token**.



- هنا ممكن تلاحظ فرق في error
- دي ممكن تكون ثغره عشان نت كذا قدرت تعمل enumeration user

```
root@team:~/wordlist/SecLists/Usernames# ffuf -u http://83.136.255.196:49534 -w xato-  
net-10-million-usernames.txt -d "username=FUZZ&password=oifjaojad" -H "Content-Type:  
application/x-www-form-urlencoded" -X POST
```

- تستعمل ffuf عشان تعمل fuzz بالطريقه دي



- دا موقع اسمه hack tricks
- بيساعدك انه يدريك حاجات تعدي بيها rate limit



- ممكن تلاقي ثغره في captha عن طريق انه هي بتكون id نفسه تعتبر ثغره

The session token is 32 characters long; thus, it seems infeasible to enumerate other users' valid sessions. However, let us send the login request multiple times and take note of the session tokens assigned by the web application. This results in the following session tokens:

```
2c0c58b27c71a2ec5bf2b4b6e892b9f9
2c0c58b27c71a2ec5bf2b4546092b9f9
2c0c58b27c71a2ec5bf2b497f592b9f9
2c0c58b27c71a2ec5bf2b48bcf92b9f9
2c0c58b27c71a2ec5bf2b4735e92b9f9
```

As we can see, all session tokens are very similar. In fact, of the 32 characters, 28 are the same for all five captured sessions.

The session tokens consist of the static string `2c0c58b27c71a2ec5bf2b4` followed by four random characters and the string `92b9f9`. This reduces the effective randomness of the session tokens. Since 28 out of 32 characters are static, there

- ممكن لو لقيت session مشتابه كذا الول اختلاف بسيط
- ممكن تفكه عادي عمله decode وتكسره